EXHIBIT 12

THE UNIVERSITY OF CHICAGO
POLICY ON INFORMATION TECHNOLOGY USE AND ACCESS

Since its inception, the University has been absolutely committed to ensuring open discourse and the free expression of viewpoints and beliefs. The commitment includes ensuring that academic dialogue is free from unwarranted institutional intrusion and oversight. With the values of open discourse and institutional restraint as guideposts, the purpose of this University-wide policy is to articulate and promote the ethical, legal, and secure use of information technology by all members of the University of Chicago community and to confirm the University's responsibilities in connection with accessing such information.

Scope

This policy applies to everyone who uses University information technology resources and to all uses of those resources, whether physically located on campus

or remotely. Although local information technology services at the University may have supplemental policies regarding acceptable use and user privacy expectations, those policies cannot diminish University responsibilities or user privacy expectations as set forth below.

Acceptable Use

The University provides information technology to its faculty, other academic appointees, postdoctoral researchers, students, staff, and some affiliates and guests to advance its educational, research, scholarship and health care missions. In addition, authorized users may also use University information technology for appropriate incidental personal use so long as those activities are legal and do not violate: University policies; contractual obligations; the safety, security, privacy, reputational, and intellectual property rights of others; or restrictions on political or commercial activities that are applicable to not for profit organizations like the University.

Every user bears the responsibility for knowing and complying with applicable laws, policies, and rules; for appropriately securing their computers and other electronic devices from misuse or theft by others; and for avoiding any use that interferes with others' legitimate access to and use of University information technology. University policies that may apply, depending on the identity of the user, include but are not limited to the University's personnel, financial and administrative policies, the Employee Handbook, the Handbook for Faculty and Other Academic Appointees, the Postdoctoral Researcher Policy Manual, the Student Manual, and any divisional, departmental, or school handbook, manual, policy or procedure, all of which are subject to change from time to time.

University Obligations

While our primary goal is to respect our users' privacy interests, the University bears significant and increasingly complex legal, operational and compliance-based duties, which from time to time require it to preserve and secure custody of

information from users' accounts and associated storage media without accessing or searching the content; in some cases, the University may also be required to access the content of user electronic information, search it using specialized software configured with appropriately tailored criteria, review the information found by the search, and disclose relevant portions to others who are duly authorized to receive it. For example, when an employee leaves the University, others often require access to the departed employee's email account to ensure continuity of business operations, research, teaching and educational programs. Likewise, the University often bears clear legal duties to preserve, review and, as appropriate, disclose data generated and/or maintained by users of University technology resources.

In this regard, the University may preserve, access, and disclose information from University information technology resources as permitted by law to uphold contractual obligations, to determine compliance with and enforce University policies and legal duties, to gather information relevant to pending or potential litigation, and to maintain the integrity and security of information technology systems. In connection with these responsibilities, the University may also be obligated to request that a user turn over or provide appropriate access to University-related information on the user's own personal computer, laptop, cell phone, or other electronic device.

In addition, when any use of University information technology presents an imminent threat to other users or to the University's technology infrastructure, or poses a likely violation of the law or University policy, the University may, without notice to the user, take whatever steps are necessary to manage the threat and/or preserve and access data. Those measures may include changing passwords, removing access rights, disabling or impounding computers, or disconnecting specific devices or entire network segments from University voice and data networks. System operators will restore connectivity and functionality as soon as practicable after they identify and neutralize the threat and implement any measures to ensure the threat does not reoccur.

Process

The University's Office of Legal Counsel (OLC) has the responsibility and authority to review and approve all requests to preserve, access, and disclose a user's electronic information. Although OLC works closely with IT Services and decision makers across the campus, its ultimate legal and ethical duties are to the institution itself.

At all times, the OLC will use reasoned judgment to determine whether requests are consistent with this policy and the law. Normally, if the request relates to accessing data maintained by academic appointees, OLC will confer with the Office of the Provost before approving, rejecting or modifying the request. Likewise, OLC will typically confer with the cognizant Dean of Students and/or the Office of the Vice President of Campus Life and Student Services before approving, rejecting or modifying requests related to data maintained by students. Human Resources will normally be consulted before approving, rejecting or modifying requests related to staff employees and volunteers. Finally, OLC will ordinarily confer with the cognizant dean's office when the request relates to other academic appointees and postdoctoral researchers. In all instances, working as needed with other units (e.g., IT Services), OLC will seek to establish conditions or other parameters for the access to data under this policy, provide a decision-making framework to allow similar requests to follow consistent process leading to similar outcomes, and maintain appropriate records of these processes. OLC will also work with IT Services to prepare an annual summary report of all such activity for the Audit Committee of the University's Board of Trustees and the University's Board of Computing and Academic Services.

Notice

In keeping with our core values, the University normally will attempt to provide advance notice to the affected individual of access to or the preservation or sharing of data with third parties unless such notification would put the University at risk or

is prohibited by law. For example, some subpoenas compel the University to obtain, preserve and produce data but forbid the University from disclosing the existence of the subpoena to the person whose data is sought. Likewise, in some misconduct investigations, the University is required to obtain and preserve research data under circumstances where advance disclosure of the data preservation may jeopardize the integrity of the investigation.

The University also maintains the authority to limit access to its networks or to remove material stored or posted on its computers when applicable policies, contractual obligations, or applicable laws are or likely have been violated.

Please see the FAQs on the Acceptable Use Policy for more information.

Category: Eligibility and Acceptable Use

Policy Owner: Chief Information Security Officer

THE UNIVERSITY OF CHICAGO

itservices@uchicago.edu

773.702.5800